NOZOMI NETWORKS

EBOOK

Cybersecurity Risk Management for Complex OT/IoT Environments

Table of Contents

1. OT/IoT Cyber Risk Can No Longer Be Ignored

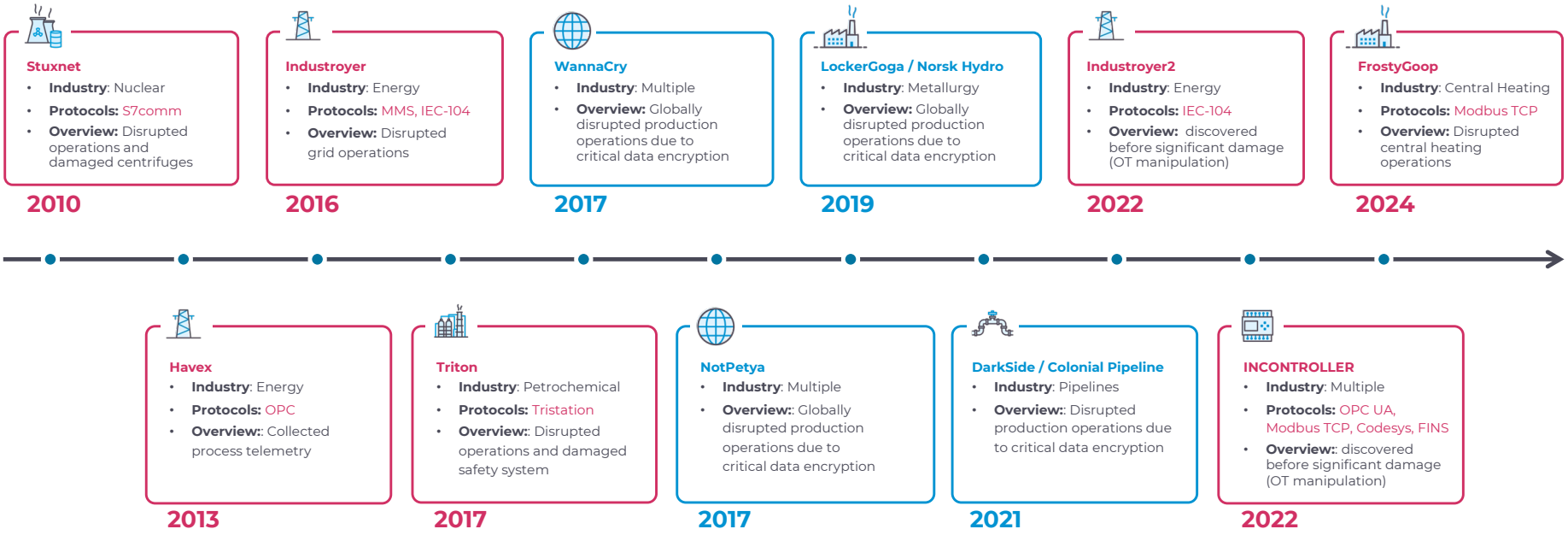
Nation-state actors, hacktivists, ransomware groups and malicious insiders... all know that global industrial environments and critical infrastructure make ideal targets. As operational technology (OT) and Internet of Things (IoT) assets account for an increasing percentage of total enterprise risk, so, too, must attention focus on reducing that risk.

By understanding the unique risks associated with industrial and critical infrastructure environments and implementing appropriate security measures, organizations can significantly reduce the likelihood and impact of both cyberattacks and operational disruptions.

Because the potential impact is so much greater in industrial environments, having the right security measures in place is critical to managing and mitigating OT/IoT cyber risk.

2. The Evolution of Cyberattacks in OT

At the same time that OT/IoT devices are accounting for a growing percentage of enterprise risk management, cyberattacks on industrial and critical environments are increasing in frequency and sophistication.



3. Managing OT/IoT Cyber Risk Requires a Different Strategy

Based on the definition alone, it's clear than managing OT/IoT cyber risk requires a different strategy than managing IT cyber risk.

What Is OT/IoT Cyber Risk?

OT/IoT cyber risk is the potential for **loss of life, injuries, equipment damage, environmental damage, revenue loss**, and operational disruptions caused by the **failure, misuse, or cyber compromise** of connected OT/IoT systems that support industrial and critical infrastructure operations.

There are four main differences between how you assess IT risk vs. OT/IoT risk:

1. Cyber and operational risk

In industrial environments we must account for both cyber and operational risk, including process risk, because operational anomalies unrelated to a cyber threat are far more common. Until investigated, you don't know whether they involve a cyberattack or not.

2. Consequence-based risk

In OT, risk assessment is almost entirely focused on consequences such as physical safety, the environment and continuity of operations — all of which impact revenue. Whether you're assessing risk in a warehouse or on a cargo ship, with OT you're always planning for your worst day.

3. Interconnected risk

Every component in an OT network is part of a larger process in a distributed environment. If one machine has a problem, you need to know what it depends on and what is depending on it. From there, what are the consequences of an emergency shutdown?

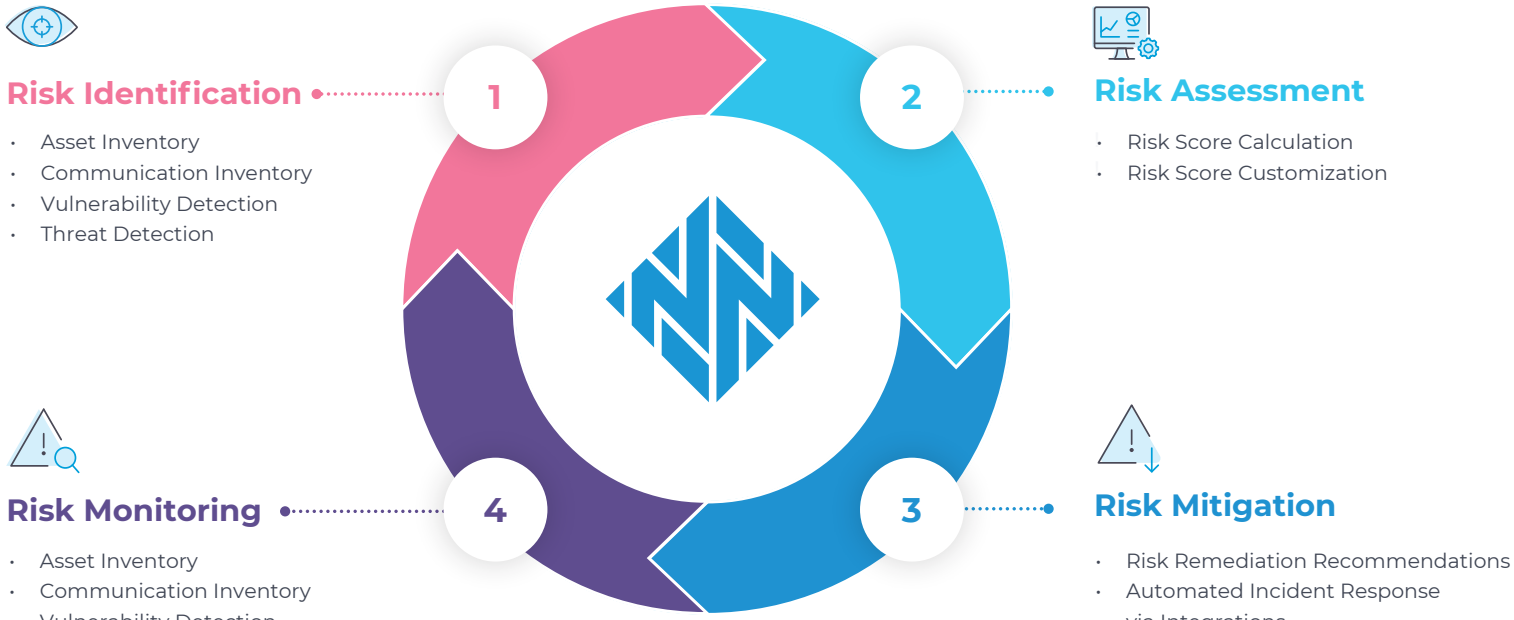
4. Vulnerabilities-only vs. multi-dimensional risk

In IT, device risk is based solely on vulnerabilities, and you can practically eliminate risk with patching. In OT, it's multilayered — and patching isn't always an option. In addition to vulnerabilities, you need to consider alert risk, communication risk, device risk, asset criticality and compensating controls.

4. The Four Steps to Continuous OT/IoT Cyber Risk Management

There are four steps to continuous OT/IoT cyber risk management: Risk Identification, Risk Assessment, Risk Mitigation and Risk Monitoring. The Nozomi Networks platform simplifies each phase in the cycle, enabling you to detect threats before they can cause harm, mitigate vulnerabilities before they can be exploited and minimize damage should an incident occur.

In doing so, it helps operators and SOC teams collaborate to prioritize efforts and take the most impactful actions to reduce risk and increase resilience.

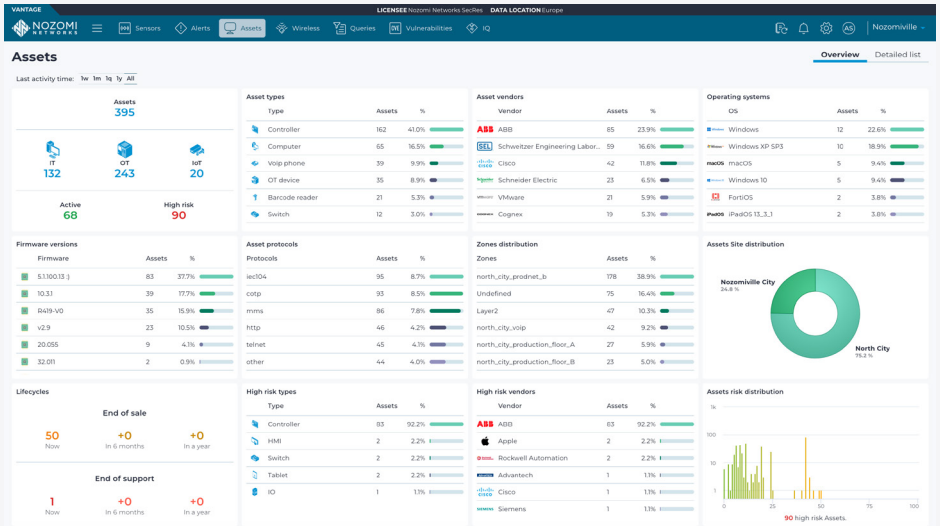


4.1 Risk Identification

A Comprehensive Asset Inventory, Turbocharged With Actionable, AI-Powered Asset Intelligence From Millions of Monitored Assets

Risk identification starts with a complete asset inventory — not just a list of IP addresses in a glorified database but full visibility into what's on your network. Nozomi Networks helps you achieve that through a variety of endpoint-to-air sensors, active and passive discovery techniques, OT/IoT protocol fluency and data ingested from leading IT security solutions.

Our AI engine learns from millions of assets that we monitor in customer environments across industries around the globe. This data trove is used to fill in gaps about identical devices across environments.



Comprehensive asset visibility through:

- Passive network monitoring
- Passive wireless network monitoring
- Active discovery packets
- Active querying
- Third-party connectors
- Threat and asset intelligence services
- Endpoint and embedded endpoint sensors

Collected asset attributes including:

- Network, user, process, software, hardware
- Utilization, lifecycle, criticality & more

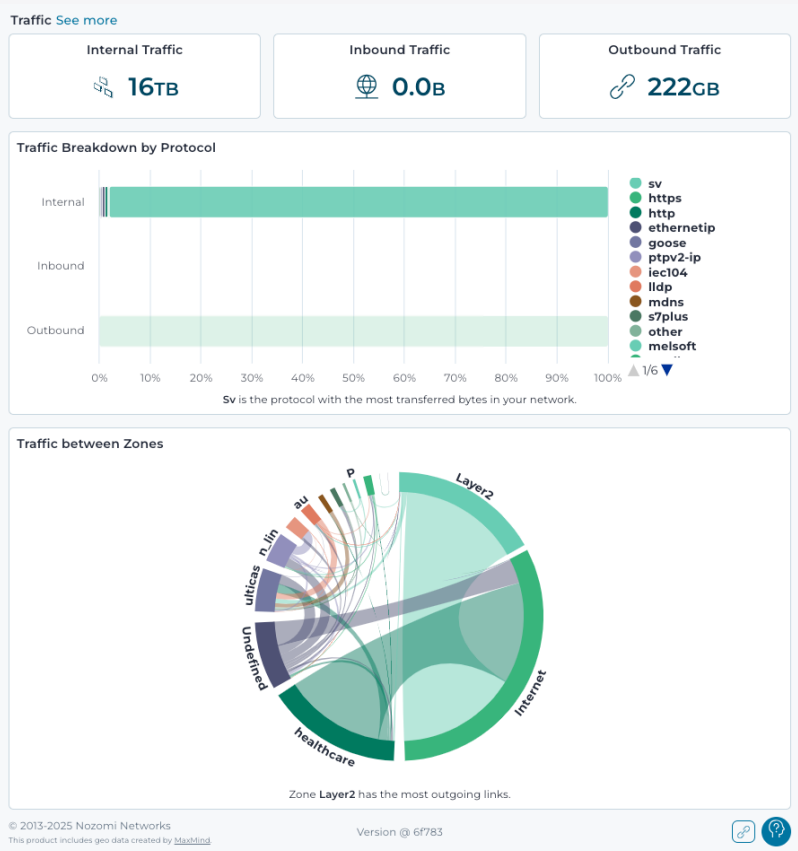
4.1 Risk Identification

Thorough Communication Inventory to Understand Asset Behavior, Including What's Communicating With What

Unlike IT devices that use standard protocols to communicate, OT systems use hundreds of protocols, many of them proprietary or industry specific — and inherently insecure — requiring deep packet inspection (DPI) to identify suspicious or anomalous behavior.

The Nozomi Networks platform understands hundreds of OT, IoT and IT protocols, from common to obscure, in both East-West and North-South communications.

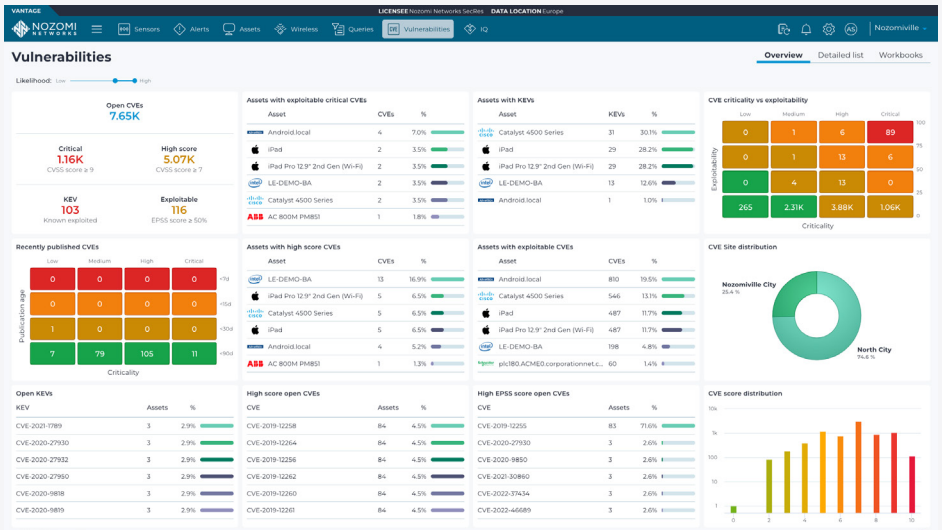
This includes authorized and unauthorized wireless communications across the 800 MHz to 5895 MHz spectrum including Wi-Fi, Bluetooth, IEEE 802.15.4, LoRaWAN, Z-Wave, cellular and drones.



4.1 Risk Identification

Vulnerability Management Prioritized Based on Criticality and Exploitability to Help You Focus on What Matters Most

Industrial networks can contain hundreds or even thousands of OT and IoT devices from a variety of vendors, many of which are insecure by design — lacking authentication, encryption and other security standards. Identifying and prioritizing critical vulnerabilities is an important component of any risk management process.



- **Automated detection and assessment of firmware,** operating system and software vulnerabilities in OT/IoT assets and communications
- **Regular updates** of vulnerability descriptions from community sources and Nozomi Networks Lab
- **Vulnerability prioritization** based on criticality and exploitability, including CVSS, EPSS and KEV scores

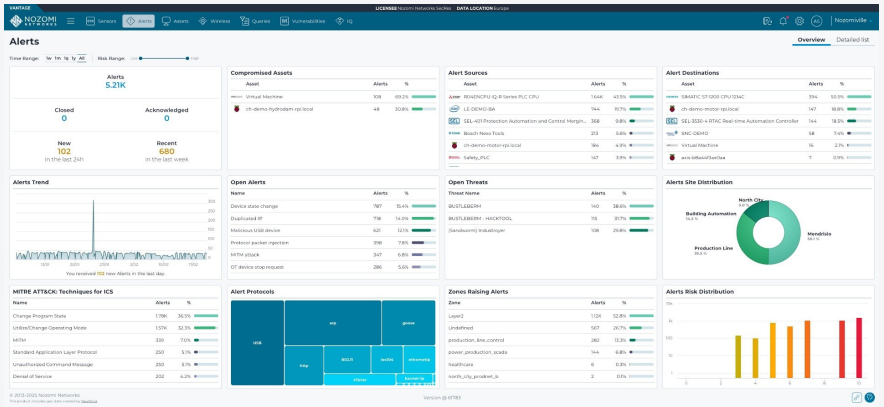
4.1 Risk Identification

AI-Driven Threat and Anomaly Detection in Network and Physical Processes That Minimizes False Positives and Alert Fatigue

Perhaps the biggest difference between IT and OT security is that in industrial environments we must account for both cyber and operational risk, including process risk. Until investigated, you don't know if an anomaly indicates an operator error or that a malicious actor has tinkered with a value. Regardless, you must be able to detect both threats and anomalies — intrusions, unwanted behavior and equipment failures —and respond quickly.

The Nozomi Networks platform has the most sophisticated detection engine available for OT/IoT environments. It combines rule-based and behavior-based techniques to detect and limit the impact of every threat in your environment, from resource spikes to living-off-the-land techniques that often evade signature-based approaches, without overwhelming analysts and operators with false positives.

To detect operational anomalies — as well as unknown threats, including zero days — the platform uses DPI to parse more than 250 industrial protocols in network traffic and extract detailed asset information. It then compares observed behavior against an AI/ML-determined baseline of your environment's normal behavior.



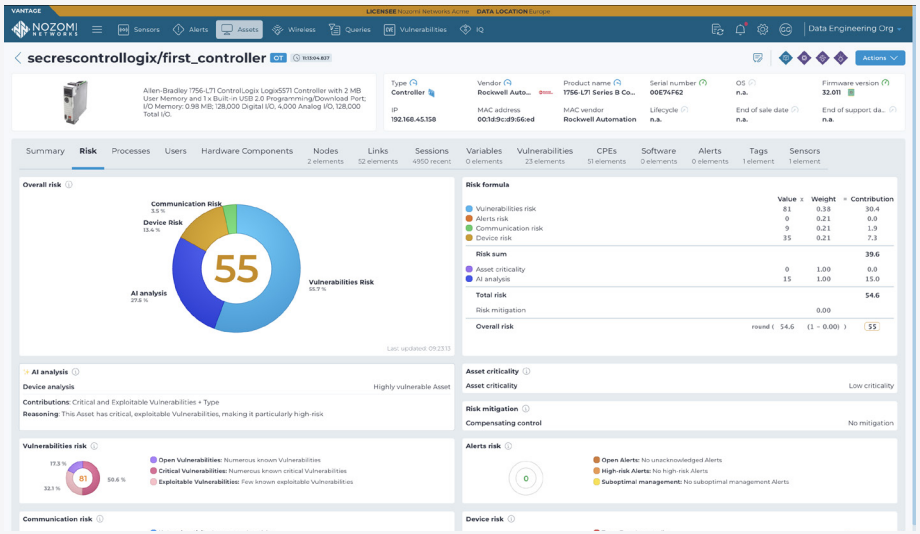
Threat detection encompassing:

- OT/IoT protocol behaviors
- Network anomalies
- Process variable anomalies
- Malicious host activities
- Wireless attacks
- Threat intelligence, including IoCs
- Custom rules

4.2 Risk Assesment

Multi-factor, AI-driven Risk Scoring, Customizable to Reflect How You Calculate Risk

When assessing OT risk, you must factor in not just vulnerabilities but also asset criticality, device risk, communication risk, alert risk and compensating controls. You can then prioritize mitigation based on asset exposure, likelihood of compromise, potential impact and organizational risk tolerance.

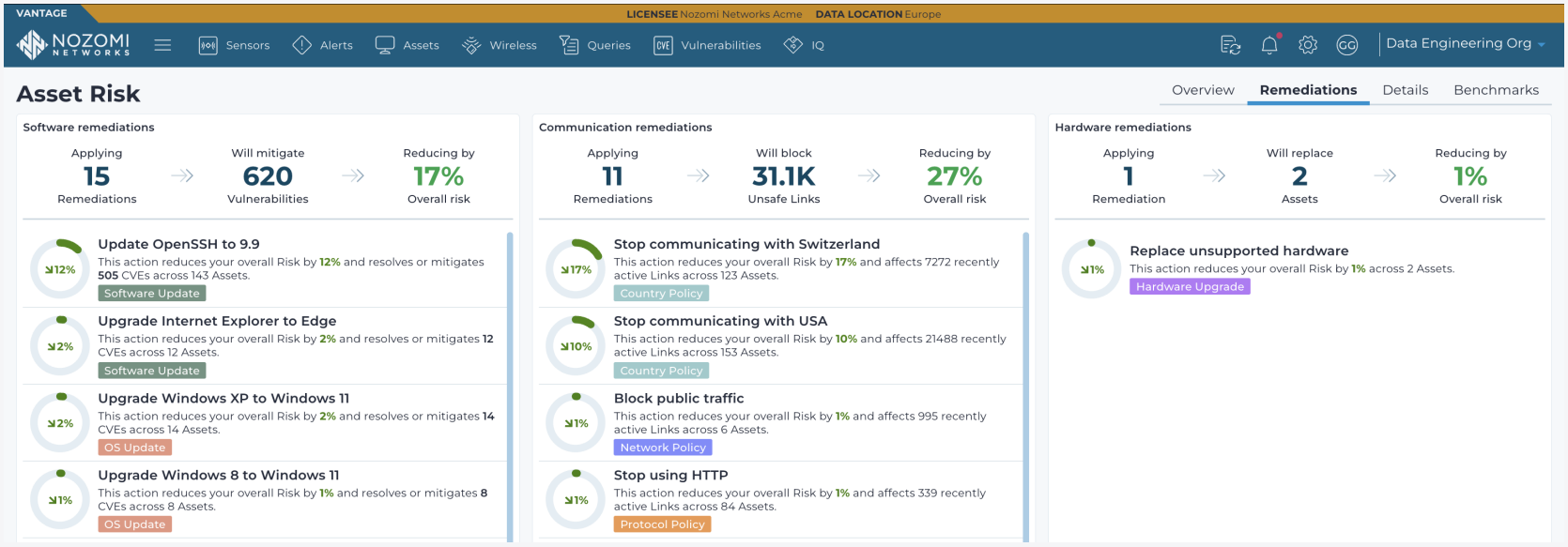


The Nozomi Networks platform assigns risk scores to each asset and related entity (sensor, zone, site, enterprise) based on these five factors. You can use these scores out of the box — or you can fully customize the weight of each variable until the calculation accurately reflects how your organization assigns risk.

4.3 Risk Mitigation

AI-driven Recommendations for Prioritized Remediation Actions

Effective OT/IoT risk remediation requires collaboration between security and operations leaders who may have different priorities. The Nozomi Networks platform leverages AI to surface key risk reduction steps that these two teams can agree will have the biggest impact. They include specific recommended actions such as patching software, fixing communication gaps and updating hardware, prioritized based their potential to reduce risk.

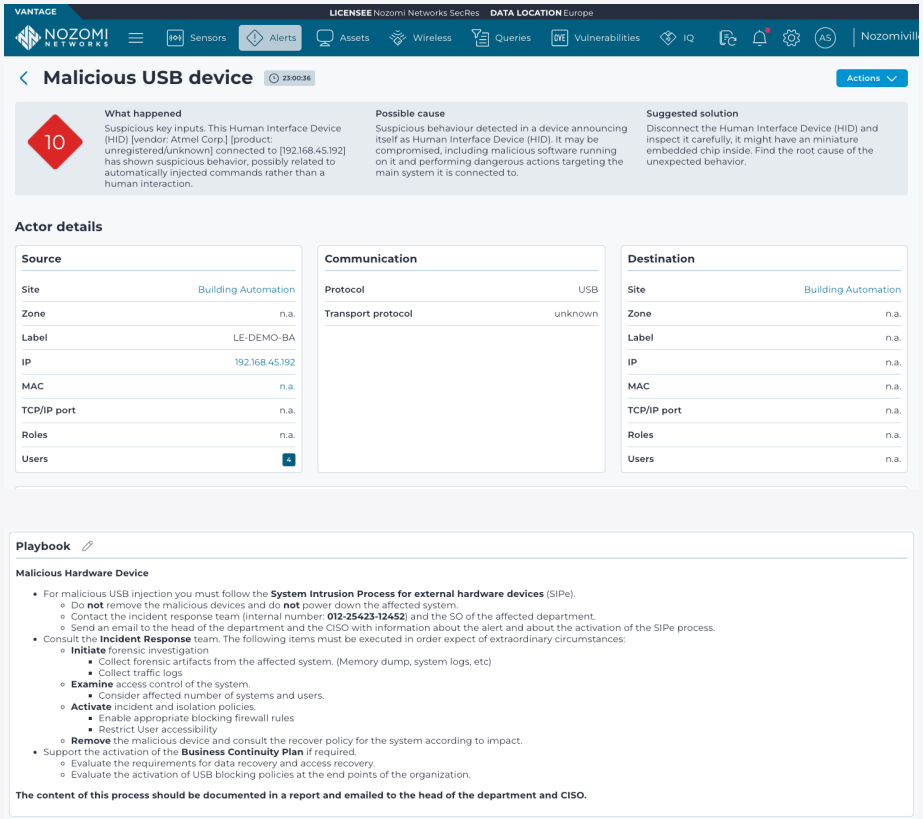


4.3 Risk Mitigation

Incident Response Guidance and Seamless Integrations for Automated Policy Enforcement

Given the premium placed on physical safety and continuous operation, incident response in industrial environments can't always be automated. The Nozomi Networks platform offers a combination of manual and automated approaches to use where appropriate:

- Customizable playbooks guide users through detailed actions to follow when an associated alert is triggered.
- Out-of-the-box integrations and OpenAPI support powers integrations with your existing tech stack, including SIEMS, SOARs, firewalls, endpoint agents, NACs, SDNs, ticketing systems, secure remote access and more.

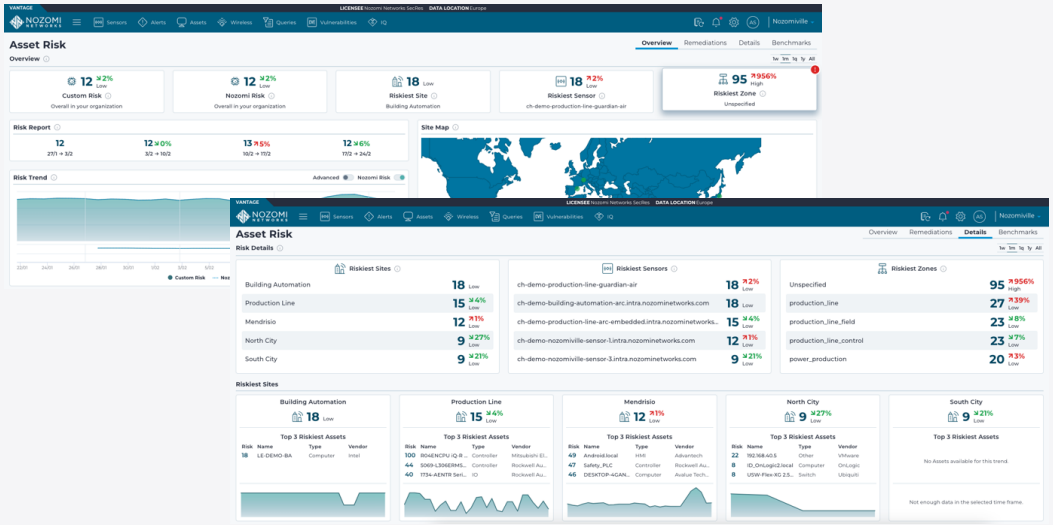


4.4 Risk Monitoring

Executive Dashboards to Monitor Risk Reduction and Benchmark Performance

Properly configured asset risk scores enable you to accurately monitor changes over time, assess how individual asset risk contributes to higher-level risk and take measures to reduce it.

Regional and industry-specific risk monitoring with actionable insights helps you shrink that risk even more.



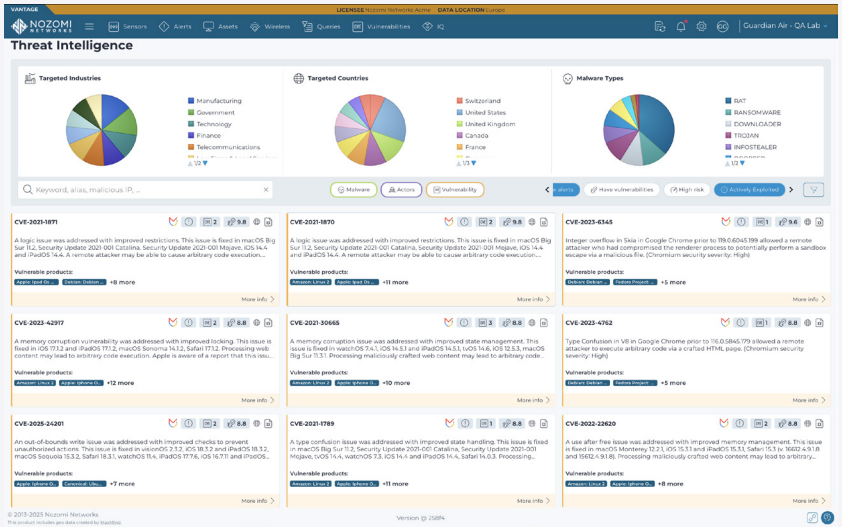
- Track **risk score changes** over time at the asset, sensor, zone, site and enterprise level
- **Benchmark your risk levels** and trends against Nozomi Networks customers in the same industry and with similar assets to your

4.4 Risk Monitoring

Comprehensive Threat Intelligence to Stay Ahead of Emerging Threats

Even as OT and IoT devices comprise a growing percentage of an organization's attack surface, there's ample evidence that most threats originate in IT networks before they spread. Especially in converged IT/OT SOCs, analysts need access to the best available threat intelligence to understand what threats are active in their industry, what techniques they use and how to detect them.

The Nozomi Networks Threat Intelligence subscription is available as a feed integrated with Mandiant threat intelligence to ensure you're aware of all known emerging threats, with key information distilled onto threat cards for quick digestion, including mitigation suggestions.



Actionable threat insights powered by Mandiant Threat Intelligence:

- Threat descriptions
- Threat activity timing
- Exploitation status and vectors
- Targeted industries and countries
- MITRE ATT&CK® details
- Mitigation suggestions and more

NOZOMI NETWORKS

NEXT STEPS

Find out how Nozomi Networks can help you see and take the most impactful actions to reduce cyber risk and increase resilience in your environment.

View Platform

Request a Demo

NOZOMI NETWORKS

Cybersecurity for OT, IoT and Critical Infrastructure

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

nozominetworks.com

NN-OT-RISK-EBOOK-001